FEE PAID
S/I

UNITED STATES DISTRICT COURT
FOR CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

VIVEK SHAH, Plaintiff, v. AMPLITUDE, INC., Defendant.	Case No.: 2:24-cv-08155-MEMF(JPRx) **COMPLAINT FOR** **(1) Violation of 18 U.S.C. § 2510, et seq.;** **(2) Violation of Cal. Penal Code § 638.51;** **(3) Violation of Cal. Penal Code § 502; and** **(4) Violation of Cal. Penal Code § 631.** **DEMAND FOR JURY TRIAL**

COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Vivek Shah ("Plaintiff" or "Shah") brings this Complaint and Demand for Jury Trial against Amplitude, Inc. ("Amplitude" or "Defendant") for surreptitiously tracking consumers' sensitive locations and capturing their in-app activities. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. Amplitude is a data analytics company that surreptitiously collects sensitive information about consumers and their mobile devices.

2. Amplitude developed and disseminated a software development kit (or "SDK") that enables backdoor access to consumers' devices and opens a data collection pipeline directly from consumers to Amplitude. Thousands of developers have embedded Amplitude's SDK into their mobile apps allowing them to siphon data from millions of consumers.

3. The data Amplitude collects from unsuspecting consumers is incredibly sensitive. Amplitude collects in-app consumer activity such as the pages they view and, in the case of shopping apps, the items they place in their shopping carts and the search terms they input. Even worse, Amplitude collects consumers' names and email addresses together with their geolocation data that reveals where a consumer lives, works, and the locations they frequent.

4. The collected location data reveals sensitive information about a consumer, for instance, their religious affiliation, sexual orientation, and medical condition allowing Amplitude to build a comprehensive profile on the consumer and their whereabouts.

5. Plaintiff is a consumer whose sensitive location data and search terms (among other in-app activities and usage) have been obtained from his devices while using ordinary mobile apps with Amplitude's SDK embedded. Plaintiff does not know—nor could he—that the apps he regularly use have embedded Amplitude's SDK and, as such, did not (and could not) consent to Amplitude's data collection practices.

PARTIES

6. Plaintiff Vivek Shah is a natural person and citizen of the State of California. He is a resident of Los Angeles, CA.

7. Defendant Amplitude, Inc is a corporation organized and existing under the laws of Delaware with its principal place of business located at 201 3rd Street, Suite 200, San Francisco, California 94103.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this matter under 28 U.S.C. § 1331.

9. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District.

10. This Court has supplemental jurisdiction over the state law claim in this action under 28 U.S.C. § 1367(a) because it is also related to the federal claims asserted against Citibank so that it forms part of the same case or controversy under Article III of the U.S. Constitution.

11. Venue is proper pursuant to 28 U.S.C. § 1391(b) because defendant resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District. According to the California Secretary of State's records, Defendant's principal place of business is located in Burbank, CA.

FACTUAL ALLEGATIONS

Amplitude Surreptitiously Collects Precise Location Information and In-App Activity from Millions of Mobile Devices

12. Amplitude is a data analytics company. Their entire business model depends on collecting sensitive information from consumers' devices and sharing it with data partners such as advertising networks and data warehouses, among others. Amplitude collects sensitive timestamped geolocation data and consumer in-app activity.

13. The secret to Amplitude's data pipeline is the collection of what the advertising industry calls "first-party data," or data collected directly from consumers. Amplitude accomplishes this task by developing a SDK.

14. SDKs are a collection of reusable and packaged pieces of computer code that perform specific functions and processes. Software developers can integrate SDKs into their applications to save time and execute specific tasks.

15. On information and belief, over 40,000 mobile app developers integrated Amplitude's SDK. These apps include, among others, shopping, productivity, dating, and gaming apps.

16. Amplitude surreptitiously collects sensitive data from consumers through its SDK in real time. Amplitude collects identity information such as the consumer's name and email address, mobile advertisings IDs ("MAIDs"), and device fingerprint data (which includes the consumer's device make and model, screen resolution, and operating system version).

17. Amplitude also collects precise and timestamped latitude and longitude geolocation coordinates from consumers' devices. This allows Amplitude to amass a database of consumers' whereabouts in real time.

18. At the forefront of Amplitude's data collection practices is obtaining consumer in-app activities in real time. Amplitude collects in-app search terms entered by the consumer, the pages requested by the consumer, and—in the case of certain shopping apps—the products the consumer viewed and the content of his or her shopping cart (collectively, the "In-App Activity").

19. Indeed, Amplitude designed its SDK to intercept the content of electronic communications between the consumer and the mobile app. Consumers entering text into a field in a mobile app or pressing a button intend to send messages to, or otherwise communicate with, the mobile app. Similarly, a mobile app rendering search results, a product page, or a web page also communicates with the consumer in response to his or her request. Amplitude's SDK collects, in real-time, the messages and/or communications intended for the mobile app such as search queries the consumer enters and sends to the mobile app service as well as the content of forms they fill out.

20. In the case of the DoorDash food delivery app, which embedded Amplitude's SDK, Amplitude collects sensitive consumer data. When logging into DoorDash, consumers can utilize the search bar to find food and/or restaurants in their area. Unbeknownst to consumers, Amplitude collects all in-app selections such as the consumer's search terms, restaurants they viewed, meals and other products they added to their shopping cart, and precise current geolocation coordinates, in real time, including the consumer's name and email address.

21. The problem with Amplitude is that consumers do not know that by interacting with an app which has embedded Amplitude's SDK that their sensitive data is being surreptitiously siphoned off by an unknown third party. Consumers are never informed about Amplitude's SDK being embedded into the app, they never consent to Amplitude's data collection practices, nor are they allowed to opt-in or opt-out of Amplitude's data collection practices—if they even know who or what Amplitude is.

22. When enabling location services within an app—for example a dating app or a shopping app that necessarily requires the consumer to share his or her location with the app—the consumer grants consent for only the mobile app to use his or her location. Similarly, consumers inputting text in an app or selecting buttons intend to communicate with the mobile app service. At no point does Amplitude inform consumers that its SDK is collecting their sensitive geolocation data and In-App Activity, nor does it prompt consumers to grant Amplitude permission to access or collect any data whatsoever.

23. In the case of DoorDash, consumers are not informed by DoorDash, Amplitude, or anyone else that Amplitude's SDK is collecting their geolocation information and In-App Activity, nor are consumers prompted to grant Amplitude permission to access or collect any data whatsoever.

24. On information and belief, a consumer would never know whether any given app has the Amplitude SDK third-party eavesdropping and tracking software embedded. The entire data collection process takes place surreptitiously without the consumer's knowledge or consent.

25. Amplitude's interception of a consumer's In-App Activity reveals information about the consumer's interests, the apps they downloaded on to their phone, preferences, and shopping histories.

Amplitude's Data Collection Reveals Sensitive Information About Consumers

26. Amplitude's practice is far from inconsequential. Its surreptitious and routine collection of precise geolocation data reveals locations associated with medical care, reproductive health, religious worship, mental health, and temporary shelters such as shelters for the homeless, domestic violence survivors, or other at-risk populations, and addiction recovery centers. As such, Amplitude's data collection may reveal, for instance, a consumer's religious affiliation, sexual orientation, medical condition, and even whether the consumer is part of an at-risk population.

27. Amplitude has also intercepted consumers' communications with mobile apps, which reveals information about a given consumer's interests, the apps downloaded onto their phone, preferences, and even shopping histories.

28. Amplitude has collected and correlated a vast amount of personal information about consumers without their knowledge and consent. Indeed, Amplitude collects information across multiple apps and identifies each consumer by a unique ID thus creating a digital dossier for the consumer, which includes information about the locations they have visited, the apps they use, their In-App Activity, and their interests, among other things.

29. To make matters worse, Amplitude has created a platform that allows the sharing of the data it harvested with even more unknown third parties. For example, Amplitude created

integrations to share data with marketing and advertising platforms such as Facebook Ads, Google Ads, TikTok Ads, and Snapchat Ads.

30. Amplitude has also developed artificial intelligence tools to analyze the data it has surreptitiously and without consent collected from consumers. Amplitude admits that it built its Artificial Intelligence tools from "over 40 trillion [consumer] events processed." Events, of course, are in-app consumer interactions such as the search terms a consumer inputs and other in-app choices.

31. Ultimately, Amplitude's SDK has allowed it to secretly create a detailed log of Plaintiff's precise movement patterns, along with a dossier of his likes and interests, all without his consent or permission.

FACTS SPECIFIC TO PLAINTIFF

32. Plaintiff downloaded and used the DoorDash food delivery and shopping app on his Android device within the last year.

33. To use the DoorDash mobile app, Plaintiff enabled location services for the sole purpose of sharing his location with DoorDash. The developers of the DoorDash mobile app have embedded the Amplitude SDK into their mobile app allowing Defendant to collect his timestamped geolocation information, device IDs, device fingerprint data, information about which app(s) he uses on his mobile device, search terms he input into the DoorDash app, the products he placed in his shopping cart, and the restaurants and products he viewed. Furthermore, Amplitude collected his name and email address and correlated his In-App Activity and geolocation information with him.

34. Plaintiff did not grant Defendant consent or permission to collect any information from his device whatsoever, let alone his precise geolocation information and In-App Activity.

35. Neither Defendant nor DoorDash informed or otherwise disclosed to Plaintiff that Amplitude's SDK was embedded in the DoorDash app, or that if he used the DoorDash app, Defendant would collect his personally identifiable information, precise geolocation information, and In-App Activity. Plaintiff did not consent to Defendant's collection.

FIRST CAUSE OF ACTION
Violation of Wiretap Act
18 U.S.C. § 2510, et seq.

36. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

37. The Wiretap Act generally prohibits the intentional "intercept[ion]" of "wire, oral, or electronic communication[s]." 18 U.S.C. § 2511(1)(a).

38. By designing the Amplitude SDK to contemporaneously and secretly collect In-App Activity—including the search terms and other text input into mobile apps by Plaintiff—Defendant Amplitude intentionally intercepted and/or endeavored to intercept the contents of "electronic communication[s]" in violation of 18 U.S.C. § 2511(1)(a).

39. Plaintiff did not consent to Defendant's collection, interception, or use of the contents of his electronic communications. Nor could he—Defendant's collection of In- App Activity is entirely without the Plaintiff's knowledge. Indeed, when Plaintiff interacted with a mobile app that embedded the Amplitude SDK, Amplitude did not announce its presence nor inform Plaintiff that it is collecting, intercepting, or using the content of the communications intended for the mobile app.

40. Furthermore, Defendant did not act as a mere extension of the mobile app used by Plaintiff because it used the intercepted communications for its own purposes. Defendant Amplitude used Plaintiff's In-App Activity to correlate data across various mobile apps to create

a unified customer profile that included Plaintiff's In-App Activity and interests. Furthermore, Defendant used Plaintiff's In-App Activity to develop and train its Artificial Intelligence.

41. Defendant never obtained any consent whatsoever from Plaintiff.

42. Plaintiff suffered harm as a result of Defendant's violations of the Wiretap Act, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(c)(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Violation of California Invasion of Privacy Act
Cal. Penal Code § 638.51

43. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

44. California law prohibits the installation of a pen register without first obtaining a court order. Cal. Penal Code § 638.51.

45. The statute defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

46. Defendant's SDK is a "pen register" because it is a device or process that records addressing or signaling information—in this instance, Plaintiff's location and personal information—from electronic communications transmitted by his devices. Furthermore, Defendant's SDK is device or process that gathers data, identifies consumers, and correlates data across various mobile apps to ascertain Plaintiff's In-App Activity and interests.

47. Defendant was not authorized by any court order to use a pen register to track Plaintiff's location and personal information, nor did it obtain consent from Plaintiff to operate such a device.

48. Plaintiff seeks injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

THIRD CAUSE OF ACTION
Violation of the California Comprehensive Computer Data Access and Fraud Act Cal. Penal Code § 502

49. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

50. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act ("CDAFA") to "expand the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). In enacting the statute, the Legislature emphasized the need to protect individual privacy: "[The] Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals[.]" Id.

51. Plaintiff's mobile devices are "computers" or "computer systems" within the meaning of Section 502(b) because they are devices capable of being used in conjunction with external files and perform functions such as logic, arithmetic, data storage and retrieval, and communication.

52. Defendant violated the following sections of CDAFA § 502(c):

a. "Knowingly accesses and without permission . . . uses any data, computer, computer system, or computer network in order to . . . wrongfully control or obtain money, property, or data." Id. § 502(c)(1).

b. "Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." Id. § 502(c)(2).

c. "Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network." Id. § 502(c)(7).

53. Defendant "accessed" Plaintiff's computers and/or computer systems because it gained entry to and/or caused output from their mobile devices to obtain geolocation information and personal information.

54. Defendant was unjustly enriched with the data it obtained from Plaintiff.

55. Plaintiff now seeks compensatory damages, injunctive relief, disgorgement of profits, other equitable relief, punitive damages, and attorneys' fees pursuant to § 502(e)(1)–(2).

FOURTH CAUSE OF ACTION
Violation of the California Wiretap Act
Cal. Penal Code § 631

56. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

57. The California Wiretap Act, Cal. Penal Code § 631, prohibits:

> Any person [from using] any machine, instrument, or contrivance, or in any other manner . . . [from making] any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or

> attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

58. Defendant's SDK intercepted Plaintiff's specific input events such as the content of their search terms, page views, button presses, and other choices on his mobile devices, including his affirmative actions (such as installing a mobile app on his device), and therefore constitute communications within the scope of the California Wiretap Act.

59. Defendant's SDK made an unauthorized connection with Plaintiff's devices and obtained his sensitive information including his movements, geolocation information, search terms, In-App Activity, mobile device IDs, device fingerprint data, and information about the mobile app(s) they downloaded.

60. Plaintiff did not consent to Defendant's collection or use of his communications. Nor could he—Defendant's collection of In-App Activity is entirely without the Plaintiff's knowledge. Indeed, when Plaintiff interacted with a mobile app that embedded the Amplitude SDK, Amplitude did not announce its presence nor inform Plaintiff that it is collecting or using the content of the communications intended for the mobile app.

61. Furthermore, Defendant did not act as a mere extension of the mobile app used by Plaintiff because it used the collected communications for its own purposes. Defendant Amplitude used Plaintiff's In-App Activity to develop and train its Artificial Intelligence systems.

62. Furthermore, Defendant attempted to and/or shared the data it wrongfully obtained from Plaintiff to third parties including advertisers and other platforms.

63. Defendant never obtained any consent whatsoever from Plaintiff.

64. Plaintiff seeks an injunction and damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

(a) An order declaring that Defendant's actions, as set out above violate the Wiretap Act, 18 U.S.C. § 2510; the California Invasion of Privacy Act, Cal. Penal Code § 638.51; the California Comprehensive Computer Data Access and Fraud Act, Cal Penal Code § 502; and the California Wiretap Act, Cal. Penal Code § 631.

(b) An injunction requiring Defendant to cease all unlawful activities;

(c) An award of liquidated damages, disgorgement of profits, punitive damages, costs, and attorneys' fees;

(d) Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Dated: September 18, 2024

Respectfully submitted,

/s/ Vivek Shah

Vivek Shah, pro se
640 S Curson Ave #1910
Los Angeles, CA 90036
(224)246-2874
newvivekshah@gmail.com